Appendix B: Proof of correctness of plan

This document is appendix B to the paper, “A First-Order Theory of Communication and Multi-Agent Plans” by E. Davis and L. Morgenstern, to appear in Journal of Logic and Computation. In this section, we prove the correctness of plan el1. Not surprisingly, the proof, though long, is neither difficult nor deep; it consists mainly of forward projections with some case splitting, combined with a good deal of definition hunting. The value of the proof is that it gives some evidence by example that the axiomatic theory is sufficient to support the kinds of inference we want out of it. In practice, the exercise of constructing the proof led to substantial improvements of various kinds in the axiomatic theory.

One particular lemmas of general interest are encountered on the way; namely, lemma B.32 proves that an agent can always follow our protocol.

Note: Axioms T.4 – T.15 define durations and clock-times to be isomorphic to the integers. We will therefore use standard results of integer arithmetic without further justification.

Temporal lemmas

(Note: lemmas B.1 — B.7 are trivial and unoriginal. However, it is easier both for the authors and for the reader to re-prove them here than to hunt them down in the literature; and their triviality means that no substantive credit is being withheld from those who have proved them before.)

Definition BD.1: Situation S1 is a successor of S0, denoted “succ(S1, S0)” if S1 follows immediately after S0.

\[ \text{succ}(S1, S0) \equiv S0 < S1 \land \neg \exists S \ (S0 < S < S1) \]

Lemma B.1: \( \text{succ}(S1, S0) \iff \text{time}(S1) = \text{time}(S0) + 1 \land S1 > S0 \).

*The research reported in this paper was supported in part by NSF grant IIS-0097537.
Proof: Right to left: Suppose that \( \text{time}(S1) = \text{time}(S0) + 1 \) and \( S1 > S0 \). By T.16, if \( S0 < SM < S1 \) then \( \text{time}(S0) < \text{time}(SM) < \text{time}(S1) \), but that is impossible. Since there can be no such \( SM \) it follows from BD.1 that \( \text{succ}(S1, S0) \).

Left to right: Suppose that \( \text{succ}(S1, S0) \). By T.16, \( \text{time}(S1) > \text{time}(S0) \); since these are integers, \( \text{time}(S1) \geq \text{time}(S0) + 1 \). By T.18, there exists \( SM \) such that \( \text{ordered}(SM, S1) \) and \( \text{time}(SM) = \text{time}(S0) + 1 \). By TD.2, T.2, T.3, \( S0 < SM \). By T.16, \( SM \leq S1 \). By definition BD.1, it cannot be the case that \( S0 < SM < S1 \). Hence, \( SM = S1 \).

Lemma B.2: \( \forall_{S0, SZ} S0 < SZ \Rightarrow \exists_S \text{succ}(S, S0) \land S \leq SZ \).

Proof: Using T.17 and T.18, let \( S1 \) be such that \( \text{time}(S1) = \text{time}(S0) + 1 \) and \( \text{ordered}(S1, SZ) \). By T.3, \( \text{ordered}(S1, S0) \). By T.16, TD.2, \( S0 < S1 \). By B.1, \( \text{succ}(S1, S0) \). By BD.1, \( S1 \leq SZ \).

Lemma B.3: \( \text{ordered}(SA, SB) \land S0 < SB \Rightarrow \text{ordered}(S0, SA) \).

Proof: By TD.2, either \( SA < SB \), \( SA = SB \) or \( SA > SB \). If \( SA < SB \), the result follows from T.3; if \( SA = SB \), the result is immediate; if \( SA > SB \), the result follows from T.2.

Lemma B.4: \( \exists_{ST} \text{time}(ST) = T \land S0 < ST < S1 \).

Proof: By T.18, there exists \( ST \) such that \( \text{ordered}(ST, S1) \) and \( \text{time}(ST) = T \). By B.3 \( \text{ordered}(ST, S0) \). By T.16, \( S0 < ST < S1 \). The uniqueness of \( ST \) follows from T.3, T.16.

Lemma B.5: (Induction from situations to intervals: Schema) Let \( \phi(S) \) be a formula with an open situation variable \( S \). Assume that the variable \( SF \) does not appear free in \( \phi \). Then the closure of the following formula holds:

\[
\left[ \phi(S0) \land \forall_S \phi(S) \Rightarrow \exists_{S1} \text{succ}(S1, S) \land \phi(S1) \right] \Rightarrow \\
\exists_I \text{start}(I) \land \forall_S \text{elt}(S, I) \Rightarrow \phi(S).
\]

Proof: Assume that the left hand of the implication holds for some \( S0 \). Let \( \Gamma(S) \) be the formula, open in \( S \), \( \forall_{S1} S0 \leq S1 \leq S \Rightarrow \phi(S) \). Then by assumption \( \Gamma(s0) \) and \( \forall_S \Gamma(S) \Rightarrow \exists_{S1} S1 > S \land \Gamma(S1) \). From axiom I.5, it follows that there exists a u-interval \( i0 \) starting in \( s0 \) in which \( \Gamma \) holds infinitely often; i.e.

\[
s0 = \text{start}(i0) \land \\
\forall_S \text{elt}(S, i0) \Rightarrow \exists_{S2} S < S2 \land \Gamma(S2) \land \text{elt}(S2, i0).
\]

Now, lest \( sa \) be any situation in \( i0 \). We have shown that \( \exists_{S2} \text{sa} < S2 \land \Gamma(S2) \); but, by definition of \( \Gamma \), that means that \( \phi(sa) \).

Lemma B.6: (Existence of a “first” situation after \( S0 \) satisfying \( \phi \)) (Schema) Let \( \phi(S) \) be a formula with an open situation variable \( S \). Assume that the variable \( SF \) does not appear free in \( \phi \). Then the closure of the following formula holds:

\[
\phi(S1) \land S0 < S1 \Rightarrow \\
\exists_{SF} \phi(SF) \land S0 \leq SF \land \forall_S S0 \leq S < SF \Rightarrow \neg \phi(S).
\]

Proof: Assume that \( S0 < S1 \) and \( \phi(S1) \). For any duration \( D \), let \( \Gamma(D) \) be the formula,

\[
\exists_{SD} \text{time}(SD) = \text{time}(S0) + D \land S0 \leq SD \leq S1 \land \phi(SD)
\]

By assumption \( \Gamma(D1) \) holds for \( D1 = \text{time}(S1) - \text{time}(S) \). Hence there is some smallest positive value \( DF \) such that \( \Gamma(DF) \). By construction of \( \Gamma \), there exists an \( SF \) such that \( \text{time}(SF) = DF, S0 < SF \).
and $\phi(SF)$. Let $S$ be any situation such that $S_0 \leq S < SF$, and let $D=\text{time}(S)-\text{time}(S_0)$. Since $D < DF$, we must have $\neg(D)$. Since $S_0 \leq S < S_1$, we must have $\neg\phi(SD)$.

**Lemma B.7:** $T_1 \geq \text{time}(\text{start}(i)) \Rightarrow \exists S_1 \text{ elt}(S_1, I) \land T_1=\text{time}(S_1)$.

**Proof:** Let $i_0$ be an interval, let $S_0=\text{start}(i_0)$, and let $t_0=\text{time}(S_0)$. Let $\Phi(D)$ be the formula “$\exists S \text{ time}(S)=t_0+D \land \text{elt}(S,i_0)$.” Clearly, since elt($S_0$,i_0), it follows that $\Phi(0)$. Suppose, inductively, that $D_1 \geq 0$ and $\Phi(D_1)$. Then there exists a situation $SX$ such that $\text{time}(SX)=t_0+D_1$ and elt($SX$,i_0). Let $S_1$ be any successor to $SX$. By I.4, there exists a situation $S_2$ such that $\neg(S_2 < S_1)$ and elt($S_2$,i_0). By T.18, there exists a situation $SM$ such that $\text{time}(SM)=t_0+D_1+1$ and ordered($SM$, $S_2$). Using T.16, it follows that in fact $SX < SM \leq S_2$, so by I.2, elt($SM$,i_0). Thus $\Phi(D_1+1)$. Using induction on durations (T.15), it follows that $\Phi(D)$ for all $D \geq 0$, which gives the desired result. Uniqueness follows from I.1 and T.16.

**Lemmas on actions and knowledge**

**Lemma B.8:**

$[\text{action}(E_1, A) \land \text{action}(E_2, A) \land \text{leads_toward}(E_1, S_0, S_1) \land \text{leads_toward}(E_2, S_0, S_2) \land \text{ordered}(S_1, S_2)] \Rightarrow E_1 = E_2$.

**Proof:** Immediate from A.1, EVD.1, AD.2, when $\text{time}(S_0) > 0t$; from A.6, AD.3 when $\text{time}(S_0)=0t$.

**Lemma B.9:** $\text{action}(E, A) \land \text{occurs}(E, S_1, S_2) \Rightarrow \text{choice}(A, S_2)$.

**Proof:** From A.2, AD.3.

**Lemma B.10:** $S_0 < S_1 < S_2 \land S_1 < SX \land \text{occurs}(E, S_0, S_2) \land \text{action}(E, A) \Rightarrow \exists SY, \text{ ordered}(SX, SY) \land \text{occurs}(E, S_0, SY)$.

(If $S_1$ is in the middle of the execution of $E$ (between $S_0$ and $S_2$) then this execution is completed along every time line that contains $S_1$.)

**Proof:** By EVD.1 leads_towards($E$, $S_0$, $S_1$). By axiom A.1, $\exists E_1 \text{ action}(E_1, A) \land \text{leads_toward}(E_1, S_0, SX)$. By EVD.1, there exists $SY$ such that $\text{occurs}(E_1, S_0, SY)$ and $\text{ordered}(SY, SX)$. By lemma B.3, $\text{ordered}(SY, S_1)$. By EVD.1, leads_towards($E_1$, $S_0$, $S_1$). But by A.1, the action of $A$ that leads from $S_0$ toward $S_1$ is unique; hence $E_1 = E$.

**Lemma B.11:**

$\forall A,S_0,S_2 \ S_0 < S_2 \Rightarrow \exists_{SY, SX, E} \ SX < S_0 < SY \land \text{action}(E, A) \land \text{occurs}(E, SX, SY) \land \text{ordered}(SY, S_2)$.

(Any situation $S_0$ occurs either at the beginning or in the middle of an action $E$ that starts in $SX$ before or at $S_0$, and that continues along every time line (toward $S_2$) containing $S_0$.)

**Proof:** If choice($A$, $S_0$) then choose $SX = S_0$. By axiom A.1 there exists an action $E$ of $A$ such that $\text{leads_toward}(E, S_0, S_2)$; that is, by EVD.1, there exists $SY$ such that $\text{ordered}(SY, S_2)$ and $\text{occurs}(E_1, S_0, SY)$.

Otherwise, if not choice($A$, $S_0$), then by AD.3 and AD.1 there exists $SX, SZ, E$ such that $\text{action}(E, A)$, $SX < S_0 < SZ$ and $\text{occurs}(E, SX, SZ)$. The result then follows from lemma B.10.

**Lemma B.12:**

$\forall A,S_0,S_2 \ S_0 < S_2 \Rightarrow \exists_{SY} \text{ choice}(A, SY) \land S_0 < SY \land \text{ordered}(SY, S_2) \land \text{time}(SY) \leq \text{time}(S_0) + \max_{\text{action}} \text{time}$.

(On any time line, choice points for $A$ occurs with a maximum gap of $\max_{\text{action}} \text{time}$.)

**Proof:** By lemma B.11, there exist $E, SX, SY$ such that $\text{action}(E, A)$, $\text{occurs}(E, SX, SY)$, $SX < S_0 < SY$ and $\text{ordered}(SY, S_2)$. By M.1, $\text{time}(SY) \leq \text{time}(SX) + \max_{\text{action}} \text{time} \leq \text{time}(S_0) +$
max action time.

**Lemma B.13:**
\[ \exists S_1 S < S_1 \wedge \text{elt}(S, I) \wedge \text{choice}(A, S_1) \wedge \text{time}(S_1) \leq \text{time}(S) + \max_{\text{action}} \text{time}. \]

**Proof:** By lemma B.7, there exists \( S_2 \) in \( I \) such that \( \text{time}(S_2) = \text{time}(S) + \max_{\text{action}} \text{time} \). The result then follows from B.12.

**Lemma B.14:** \( k_{\text{acc}}(A, S_0, S_0A) \Rightarrow \text{time}(S_0) = \text{time}(S_0A) \).

**Proof** by contradiction. Suppose this is false. Since \( k_{\text{acc}} \) is symmetric by axiom K.3, there exists \( A, S_0, S_0A \) for which \( k_{\text{acc}}(A, S_0, S_0A) \) and \( \text{time}(S_0) < \text{time}(S_0A) \). Let \( t_1 \) be the earliest time for which there exists \( a, a_1, s_1a \) such that \( k_{\text{acc}}(a, s_1, s_1a) \) and \( t_1 = \text{time}(s_1) < \text{time}(s_1a) \). Using T.18, choose an \( sa \) such that \( \text{time}(sa) = t_1, sa < s_1a. \) Using K.3, K.4 there exists a situation \( s \) such that \( k_{\text{acc}}(a, sa, s), s < s_1. \) By T.16, \( \text{time}(s) < \text{time}(s_1). \) But then, by K.3, we have \( k_{\text{acc}}(a, sa, sa) \) and \( \text{time}(s) < \text{time}(sa) = t_1, \) contradicting the assumption that \( t_0 \) was the earliest time when this could happen.

**Lemma B.15:** \( k_{\text{acc}}(A, SXA, SXB) \wedge \text{occurs}(E, SXA, SYA) \wedge \text{action}(E, A)) \Rightarrow \exists SYB \text{ occurs}(E, SXB, SYB). \)

**Proof:** By K.5, there exists \( S_1B, S_2B \) such that \( k_{\text{acc}}(A, SXA, S_1B), S_1B \leq SXB, \) and \( \text{occurs}(E, S_1B, S_2B). \) By lemma B.14, there exists \( S_2A \) such that \( \text{time}(SXA) = \text{time}(SX) = \text{time}(S_1B). \) By TD.3, T.10, T.16, \( SXB = S_1B. \)

**Lemma B.16:** \( \text{choice}(A, S_1) \wedge k_{\text{acc}}(A, S_1, S_1A) \Rightarrow \text{choice}(A, S_1A). \)

(You know when you’re at a choice point.)

**Proof:** By AD.1 and AD.2, there exist \( E, S_2 \) such that \( \text{action}(E, A) \) and \( \text{occurs}(E, S_1, S_2). \) By lemma B.15 there exists \( S_2A \) such that \( \text{occurs}(E, S_1A, S_2A). \) By AD.1, AD.2 \( \text{choice}(A, S_1A). \)

**Lemma B.17:** \( \forall_S A k_{\text{acc}}(A, S, SA) \Rightarrow \text{choice}(A, SA) \) \( \lor \) \( \forall_S A k_{\text{acc}}(A, S, SA) \Rightarrow \neg \text{choice}(A, SA) \).

(You know whether you’re at a choice point.)

**Proof:** Immediate from K.2 and lemma B.16.

**Lemma B.18:**
\[ [\text{action}(E, A) \wedge k_{\text{acc}}(A, S_0, S_0A) \wedge \text{feasible}(E, S_0)] \Rightarrow \text{feasible}(E, S_0A). \]

**Proof:** By EVD.2 there exists \( S_1 \) such that \( \text{occurs}(E, S_0, S_1). \) By lemma B.15, there exists \( S_1A \) such that \( \text{occurs}(E, S_0A, S_1A). \) By EVD.2, \( \text{feasible}(E, S_0A). \)

**Lemma B.19:**
\[ k_{\text{acc}}(A, S, SA) \wedge \text{action}(E, A)) \Rightarrow [\text{engaged}(E, A, S) \Leftrightarrow \text{engaged}(E, A, SA)]. \]

(You know whether you’re engaged in action \( E. \))

**Proof:** From axioms AD.1 and K.5.

**Definition BD.2:** \( \text{know}_{\text{whether}}(A, Q, S) = \)
\[ \forall_S A k_{\text{acc}}(A, S, QA) \Rightarrow \text{holds}(SA, Q) \] \( \lor \) \[ \forall_S A k_{\text{acc}}(A, S, SA) \Rightarrow \neg \text{holds}(SA, Q) \]

(\( A \) knows whether \( Q \) holds in \( S \) means that either \( A \) knows in \( S \) that \( Q \) holds in \( S \) or \( A \) knows in \( S \) that \( Q \) does not hold in \( S. \))

**Definition BD.3:**
\[ k_{\text{acc}_\text{int}}(A, S_1, S_2, S_1A, S_2A) = k_{\text{acc}}(A, S_1, S_1A) \wedge k_{\text{acc}}(A, S_2, S_2A) \wedge S_1 < S_2 \wedge S_1A < S_2A. \]

(Interval \([S_1A, S_2A]\) is knowledge accessible from \([S_1, S_2].\))
Lemma B.20:
\[ \forall S \ know \ whether(AC, Q, S) \Rightarrow \]
\[ \forall S_{0,A,S_{1,A}} [ k_{acc \ int}(AC, S_{0}, S_{1}, S_{0,A}, S_{1,A}) \Rightarrow \text{opportunity}(S_{1,A}, AC, AR, Q)] \lor \]
\[ \forall S_{0,A,S_{1,A}} [ k_{acc \ int}(AC, S_{0}, S_{1}, S_{0,A}, S_{1,A}) \Rightarrow \neg \text{opportunity}(S_{1,A}, AC, AR, Q)] \]
(If AC always knows whether Q is true, then he always know whether S1 is an opportunity to act on Q.)

Proof: From MD.2, lemma B.17, and lemma B.14.

Lemma B.21:
\[ \forall S \ know \ whether(AC, Q, S) \Rightarrow \]
\[ \forall S_{0,A,S_{1,A}} [ k_{acc \ int}(AC, S_{0}, S_{1}, S_{0,A}, S_{1,A}) \Rightarrow \text{first \ opportunity}(S_{1,A}, AC, AR, S_{0,A}, Q)] \lor \]
\[ \forall S_{0,A,S_{1,A}} [ k_{acc \ int}(AC, S_{0}, S_{1}, S_{0,A}, S_{1,A}) \Rightarrow \neg \text{first \ opportunity}(S_{1,A}, AC, AR, S_{0,A}, Q)] \]
(If AC always knows whether Q is true, then he always know whether S1 is the first opportunity to act on Q.)


Lemmas about plans

Lemma B.22: \begin{plan}(P, AC, AR, S_{0}, S_{1}) \land S_{0} \leq S_{M} < S_{1} \Rightarrow \begin{plan}(P, AC, AR, S_{0}, S_{M}).

Proof: From QD.6

Lemma B.23: \text{attempt \ toward}(P, AC, AR, S_{0}, S_{1}) \land S_{0} \leq S_{M} < S_{1} \Rightarrow \text{attempt \ toward}(P, AC, AR, S_{0}, S_{M}).

Proof: Assume that \text{attempt \ toward}(p,ac,ar,s0,s1) and that s0≤sm<s1. By QD.8, either \begin{plan}(p,ac,ar,s0,s1) or for some s2 between s0 and s1, \begin{plan}(p,ac,ar,s0,s2) and terminates\plan(p,ac,ar,s0,s2). There are three cases to consider:

Case 1: \begin{plan}(p,ac,ar,s0,s1). By lemma B.22, \begin{plan}(p,ac,ar,s0,sm). By QD.8, \text{attempt \ toward}(p,ac,ar,s0,sm).

Case 2: \begin{plan}(p,ac,ar,s0,s2), terminates\plan(p,ac,ar,s0,s2), and sm≥s2. Then, by QD.8, \text{attempt \ toward}(p,ac,ar,s0,sm).

Case 3: \begin{plan}(p,ac,ar,s0,s2), terminates\plan(p,ac,ar,s0,s2), and sm<s2. Then, by lemma B.22, \begin{plan}(p,ac,ar,s0,sm), so by QD.8, \text{attempt \ toward}(p,ac,ar,s0,sm).

Lemma B.24:
\begin{plan}(P, AC, AR, S_{0}, S_{1}) \land \text{choice}(AC, S_{1}) \land \neg \text{terminates}(P, AC, AR, S_{0}, S_{1})\land \text{know \ next \ step}(E, P, AC, S_{0}, S_{1}) \land \text{leads \ towards}(E, S_{1}, S_{2}) \land \text{succ}(S_{2}, S_{1}) \Rightarrow \begin{plan}(P, AC, AR, S_{0}, S_{2})

Proof: This together with lemma B.25 are, so to speak, the recursive restatement of definition QD.6. That is, these two lemmas define \begin{plan}(P \ldots S_{2}) recursively in terms of \begin{plan}(P \ldots S_{1}) where S_{1} is the predecessor of S_{2}.

Assume that the left-hand side of the above implication holds. By QD.6, since \begin{plan}(P, AC, AR, S_{0}, S_{1}) we have S_{0} \leq S_{1}. Since succ(S_{2}, S_{1}) it follows that S_{0} < S_{2}.

For any intermediate situation SM and for a final situation SZ either equal to S1 or S2, let us abbreviate the condition
\[ \neg \text{terminates}(P, AC, AR, S_{0}, S_{M}) \land \]
on the right-hand side of QD.6 as $\Phi_{P,AC,AR,S0}(SM,SZ)$. By QD.6, we know that $\Phi(SM,S1)$ holds for all $SM$ such that $S0 \leq SM < S1$. Also by QD.6, if we can establish that $\Phi(SM,S2)$ holds for all $SM$ such that $S0 \leq SM < S2$, then we have established the desired result begin_plan($P,AC,AR,S0,S2$). There are three cases:

Case 1: $S0 \leq SM < S1$ and choice($AC,SM$). Since $\Phi(SM,S1)$, there exists $E$ such that know_{next_step}(E,P,AC,S1,SM) and leads_towards(E,SM,S1). By assumption, we have choice($AC,S1$). Therefore the condition leads_towards($E,SM,S1$) implies that occurs($E,SM,SN$) for some $SN \leq S1 < S2$, so we have leads_towards($E,SM,S2$). Thus we have established all parts of $\Phi(SM,S2)$.

Case 2: $S0 \leq SM < S1$ and $\neg$choice($AC,SM$). Thus, in this case $\Phi(SM,S2)$ requires only that $\neg$terminates($P,AC,AR,S0,SM$), which we know from $\Phi(SM,S1)$.

Case 3: $SM = S1$. $\Phi(S1,S2)$ is explicitly stated on the left side of the implication in the statement of our lemma.

\textbf{Lemma B.25:}
\begin{align*}
\text{[begin_plan}(P,AC,AR,S0,S1) \land \neg\text{choice}(AC,S1) \land \\
\neg\text{know\_succeeds}(P,AC,S0,S1) \land \text{succ}(S2,S1)] \Rightarrow \text{begin\_plan}(P,AC,AR,S0,S2).
\end{align*}

\textbf{Proof:} By QD.3, QD.4, QD.5, $P$ can only terminate in $S1$ if either choice($AC,S1$) or know\_succeeds($P,AC,S0,S1$). The result then follows from QD.6.

\textbf{Lemma B.26:}
\begin{align*}
\text{[begin\_plan}(P,AC,AR,S0,S1) \land S0 \leq SM < S1 \land \text{leads\_towards}(E,SM,S1) \land \text{action}(E,AC)] \Rightarrow \\
\text{know\_next\_step}(E,P,AC,S0,SM).
\end{align*}

\textbf{Proof:} By EVD.1, AD.2, and AD.3, choice($AC,SM$). By QD.6, there is an action $E1$ in $SM$ which $A$ knows to be a next step of $P$ and which leads toward $S1$. By P.1, $E1$ is an action of $AC$. By A.1, $E1 = E$. Hence, $AC$ knows in $SM$ that $E$ is a next step of $P$.

\textbf{Lemma B.26.A:} $\forall S1,S2 \ S1 < S2 \land \text{soc\_poss}(S2) \Rightarrow \text{soc\_poss}(S1)$.

\textbf{Proof:} From QD.9 and lemma B.23.

\textbf{Lemma B.27:}
\begin{align*}
[D1 \geq 0 \land D2 \geq 0 \land T \leq T2 \leq T + D1 \land \text{reserved\_block}(T,AC,AR,D1 + D2)] \Rightarrow \\
\text{reserved\_block}(T2,AC,AR,D2).
\end{align*}

\textbf{Proof:} From QD.1 with arithmetic.

\textbf{Lemma B.28:} [working\_on($P,AC,AR,S0,S1$) $\land S0 \leq SB \leq S1] \Rightarrow \text{working\_on}(P,AC,AR,S0,SB)$.

\textbf{Proof:} From Q.5, QD.6, and lemma B.22.

\textbf{Lemma B.29:}
\begin{align*}
\text{[working\_on}(PX,AC,AR,SX,S) \land \text{working\_on}(PY,AC,AR,SY,S)] \Rightarrow PY = PX \land SY = SX.
\end{align*}

Agent $AC$ works on at most one plan of agent $AR$’s at a time.

\textbf{Proof:} From Q.5, we have $SX \leq S$, accepts\_req($PX,AC,AR,SX$), $SY \leq S$, accepts\_req($PY,AC,AR,SY$).
By T.3, either $SX \leq SY$ or $SY \leq SX$. Assume without loss of generality that $SX \leq SY$. By
Lemma B.28: working\textunderscore on\((PX, AC, AR, SX, SY)\). By Q.6 since accepts\textunderscore req\((PY, AC, AR, SY)\), it follows that \(\forall_{PQ, SQ} \text{working\textunderscore on}(PQ, AC, AR, SQ, SY) \Rightarrow PQ = PY, SQ = SX\). Hence \(PX = PY, SX = SY\).

Lemma B.30
\[
[\text{working\textunderscore on}(P, AC, AR, S0, S1) \land \text{action}(E, AC) \land S0 \leq SM \land \text{leads\textunderscore toward}(E, SM, S1)] \Rightarrow \text{know\textunderscore next\textunderscore step}(E, P, AC, S0, SM).
\]


Lemma B.31
\[
[\neg\exists_{S0} \text{working\textunderscore on}(P, AC, AR, S0, S1)] \land \text{working\textunderscore on}(P, AC, AR, S2, S3) \land S1 < S3 \Rightarrow S1 < S2 \land \exists_{SX} \text{occurs}\textunderscore request}(AC, AR, P, SX, S2).
\]

(If \(AC\) goes from not working on \(P\) in \(S1\) to working on \(P\) from \(S2\) to \(S3\), then a request to do \(P\) must have completed at \(S2\).)

Proof: Since working\textunderscore on\((P, AC, AR, S2, S3)\), by Q.5 accepts\textunderscore req\((P, AC, AR, S2)\). By lemma B.28, for all \(SB\) between \(S2\) and \(S3\), working\textunderscore on\((P, AC, AR, S2, SB)\). Hence \(S1\) is not between \(S2\) and \(S3\), so \(S1 < S2\). By Q.6 there exists an \(SX\) such that occurs\textunderscore request\((P, AC, AR, SX, S2)\).

Definition BD.4.: good\textunderscore action\((E, AC, S1) \equiv \text{choice}(AC, S1) \land \forall_{P, AR, S0} [\text{working\textunderscore on}(P, AC, AR, S0, S1) \Rightarrow \text{know\textunderscore next\textunderscore step}(E, P, AC, AR, S0, S1)].

Action \(E\) is a good action for \(AC\) in \(S1\) if it is a continuation of every plan \(P\) that \(AC\) is currently working on.

Lemma B.32: \(\forall_{AC, S} \text{choice}(AC, S) \Rightarrow \exists_{E} \text{good\textunderscore action}(E, AC, S).

“There is one thing, Emma, that a man can always do if he chooses, and that is, his duty.”

(Jane Austen)

Proof: A hierarchical case analysis

Case 1. Suppose there exist \(AR, P, S0\) such that \(AC\) reserves \(time(S)\) for \(AR\) and working\textunderscore on\((P, AC, AR, S0, S)\).

By axiom Q.1 and lemma B.29 there is at most one such \(AR, P, S0\).

Case 1.1: Suppose there is an action \(E\) such that exec\textunderscore cont\((E, P, AC, AR, S0, S)\).

By QD.2, know\textunderscore next\textunderscore step\((E, P, AC, AR, S0, S)\). Let \(PX \neq P, ARX, S0X\) be any values such that working\textunderscore on\((PX, AC, ARX, S0X, S)\). By lemma B.29, \(ARX \neq AR\), so by Q.1, \(\neg\text{reserved}(time(S), AC, ARX)\). By QD.2 \(\neg\text{governs}(ARX, E)\) and by PD.1 feasible\textunderscore \((E, S)\).

Since working\textunderscore on\((PX, AC, ARX, S0X, S)\), by Q.5 \(\neg\text{terminates}(PX, AC, ARX, S0X, S)\).

By QD.5 \(\neg\text{abandon2}(P, AC, ARX, S0X, S)\). By QD.4, for any action \(E1\), if action\textunderscore \((E1, AC)\) and \(\neg\text{governs}(ARX, E1)\) then know\textunderscore next\textunderscore step\((E1, P, AC, ARX, S0X, S)\). In particular know\textunderscore next\textunderscore step\((E, P, AC, S0X, S)\).

Since the implication “working\textunderscore on\((PX, AC, ARX, S0X, S) \Rightarrow \text{know\textunderscore next\textunderscore step}(E, PX, AC, S0X, S)\)” holds for all \(PX, ARX, S0X\), we have good\textunderscore action\((E, AC, S)\) (definition BD.4).

Case 1.2 Suppose that there is no action \(E\) such that exec\textunderscore cont\((E, P, AC, AR, S0, S)\). By QD.3, abandon1\((P, AC, AR, S0, S)\). By QD.5, terminates\((P, AC, AR, S0, S)\). But by Q.5 this contradicts the assumption that working\textunderscore on\((P, AC, AR, S0, S)\).

Case 2. Suppose that reserved\textunderscore \((time(S), AC, AR)\) and choice\textunderscore \((AC, S)\), but there is no plan \(P\) and situation \(S0\) such that working\textunderscore on\((P, AC, AR, S0, S)\). Let \(E = \text{do(AC, wait)}\), so \(E\) is not governed by any agent (Q.4). Let \(PX, ARX, S0X\) be any values such that working\textunderscore on\((PX, AC, ARX, S0X, S)\).

Then we can prove that know\textunderscore next\textunderscore step\((E, PX, AC, S0X, S)\) using exactly the same argument as in case 1.1.
Case 3. Suppose that time(S) is not reserved for any agent AR. Let $E = \text{do}(AC, wait)$, so $E$ is not governed by any agent (Q.4). Let $PX, ARX, S0X$ be any values such that $\text{working}(PX, AC, ARX, S0X, S)$. Then, again, we can prove that $\text{know}_\text{next} \text{step}(E, PX, AC, ARX, S0X, S)$ using exactly the same argument as in the second part of case 1.1. □

**Lemma B.33:** $\text{soc} \_ \text{poss}(S1) \land S < S1 \land \text{leads} \_ \text{towards}(E, S, S1) \land \text{action}(E, AC) \Rightarrow \text{good} \_ \text{action}(E, AC, S)$.

(If a "socially possible" history, all actions are good.)

**Proof:** Assume that the left-hand side of the implication is satisfied. We need to prove that $\text{good} \_ \text{action}(E, AC, S)$; that is, by definition BD.4,

$$\text{choice}(AC, S) \land \forall_{P, AR, S0} \text{working}(P, AC, AR, S0, S) \Rightarrow \text{know}_\text{next} \text{step}(E, P, AC, S0, S)$$

It is immediate from AD.2, EVD.2 that $\text{choice}(AC, S)$. Assume that $\text{working}(P, AC, AR, S0, S)$.

Clearly $S0 \leq S < S1$. By Q.5 we have $\text{accepts}_\text{req}(P, AC, AR, S0)$, $\text{begin}_\text{plan}(P, AC, AR, S0, S)$ and $\neg \text{terminates}(P, AC, AR, S0, S)$. By QD.8, $\text{attempt}_\text{toward}(P, AC, AR, S0, S)$. Since $\text{begin}_\text{plan}(P, AC, AR, S0, S)$, by QD.6 $\forall_{SM} S0 \leq SM < S \Rightarrow \text{terminates}(P, AC, AR, S0, SM)$. Since $\text{leads} \_ \text{towards}(E, S, S1)$ there exists $S2$ such that $\text{occurs}(E, S, S2)$ and $\text{ordered}(S2, S1)$. Let $S4$ be such that $\text{succ}(S4, S)$ and $S4 \leq S2$. Clearly $S4 \leq S1$. By lemma B.26.A, $\text{soc} \_ \text{poss}(S4)$. By QD.9 $\text{attempt}_\text{toward}(P, AR, AC, S0, S4)$. But we have, for all $SM$ such that $S0 \leq SM < S$, $\neg \text{terminates}(P, AC, AR, S0, SM)$. Hence by QD.8, $\text{begin}_\text{plan}(P, AC, AR, S0, S4)$. Since $E$ is the unique action such that $\text{leads} \_ \text{toward}(E, S0, S4)$, it follows from QD.6 that $\text{know}_\text{next} \text{step}(E, P, AC, S0, S)$.

**Lemma B.34:**

$\forall_{S, AC, E} [S < S1 \land \text{action}(E, AC) \land \text{leads} \_ \text{towards}(E, S, S1)] \Rightarrow \text{good} \_ \text{action}(E, AC, S)] \Rightarrow \text{soc} \_ \text{poss}(S1).

(If all actions before $S1$ are good, then $S1$ is socially possible.)

**Proof** of the contrapositive: Suppose that $\neg \text{soc} \_ \text{poss}(S1)$. By QD.9, there exist $S0, P, AC, AR$ such that $S0 < S1$, $\text{accepts}_\text{req}(P, AC, AR, S0)$ and $\neg \text{attempt}_\text{toward}(P, AC, AR, S0, S1)$. By QD.8 $\neg \text{begin}_\text{plan}(P, AC, AR, S0, S1)$. By QD.6 $\text{begin}_\text{plan}(P, AC, AR, S0, S0)$. Let $S3$ be the last situation such that $S0 \leq S3 < S1$ and $\text{begin}_\text{plan}(P, AC, AR, S0, S3)$. Since $\neg \text{attempt}_\text{toward}(P, AC, AR, S0, S1)$, it follows from QD.8 that $\neg \text{terminates}(P, AC, AR, S0, S3)$; and from QD.5 that $\neg \text{know} \_ \text{succeeds}(P, AC, AR, S0, S3)$. From lemma B.25 it follows that $\text{choice}(AC, S3)$. From Q.5 we have $\text{working}(P, AC, AR, S0, S3)$. Let event $E$ be such that $\text{leads} \_ \text{toward}(E, S3, S1)$, and suppose that $\text{occurs}(E, S3, S4)$, where $\text{ordered}(S4, S1)$. Let $S5$ be the earlier of $S1$ and $S4$; then $S3 < S5 \leq S1$.

Since we defined $S3$ to be the last situation such that $S0 \leq S3 < S1$ and $\text{begin}_\text{plan}(P, AC, AR, S0, S3)$, it follows that $\neg \text{begin}_\text{plan}(P, AC, AR, S0, S5)$. By the contrapositive to lemma B.24, $E$ must not be a continuation of $P$ in $S3$; hence, by definition BD.4, $E$ is not a good action in $S3$. Thus, we have established that if $\neg \text{soc} \_ \text{poss}(S1)$ then there exist $E, S3, P, AC$, such that $S3 < S1$, $\text{action}(E, AC)$, $\text{leads} \_ \text{towards}(E, S3, S1)$, and $\neg \text{good} \_ \text{action}(E, AC, S3)$, which is just the contrapositive of the statement of the lemma.

**Lemma B.35:** $\text{soc} \_ \text{poss}(S1) \Leftrightarrow \\
\forall_{S, AC, E} [S < S1 \land \text{action}(E, AC) \land \text{leads} \_ \text{towards}(E, S, S1)] \Rightarrow \text{good} \_ \text{action}(E, AC, S)$.

($S1$ is socially possible if and only if all actions before $S1$ are good.)

**Proof:** From B.33 and B.34.

**Lemma B.36:**

$[\text{accepts}_\text{req}(P, AC, AR, S0) \land S1 > S0 \land \text{soc} \_ \text{poss}(S1)] \Rightarrow \\
[\text{working}(P, AC, AR, S0, S1) \lor \\
$
\[\exists SM \ 0 \leq SM \leq S1 \land \text{beginplan}(P, AC, AR, S0, SM) \land \text{terminates}(P, AC, AR, S0, SM)]\.

**Proof:** Assume that the left-hand side of the implication holds. By QD.9, attempt\_toward\((P, AC, AR, S0, S1)\). By QD.8, either \(P\) begins over the interval \([S0, S1]\) or it finishes over some initial segment \([S0, SM]\). The second possibility is the second disjunct of the right-hand side of our lemma. If \(P\) does not finish over \([S0, S1]\) initial segment and \(P\) begins over \([S0, S1]\) then by Q.5 \(AC\) is working on \(P\) in \(S1\).

**Lemma B.37:** \(\text{soc}\_\text{poss}(S0) \Rightarrow \exists S1 \ \text{succ}(S1, S0) \land \text{soc}\_\text{poss}(S1)\).

**Proof:** Assume that \(\text{soc}\_\text{poss}(S0)\). If \(S0\) is a choice point for agent \(A\), then using lemma B.32, let \(E\) be an action such that good\_action\((E, A, S)\) and let \(S1\) be a situation such that leads\_towards\((E, S, S1)\) and \(\text{succ}(S1, S)\). If \(S\) is not a choice point for any agent \(A\), let \(S1\) be any situation such that \(\text{succ}(S1, S)\). By B.35, since \(\text{soc}\_\text{poss}(S0)\), all actions before \(S0\) are good actions; by the above constructions, the action, if any, at \(S0\) is a good action. Thus, all actions before \(S1\) are good actions, so by lemma B.35, \(\text{soc}\_\text{poss}(S1)\).

**Lemma B.38** \(\text{soc}\_\text{poss}(S) \Rightarrow \exists I \, S=\text{start}(I) \land \text{soc}\_\text{poss}\_\text{int}(I)\).

(Any \(\text{soc}\_\text{poss}\) situation \(S\) can be extended to an unbounded \(\text{soc}\_\text{poss}\) interval \(I\).)

**Proof:** From lemmas B.37 and B.5.

**Validation of plan el2**

**Lemma B.39:**
\(\text{know}\_\text{acc}(A, S1, S1A) \land T0 < \text{time}(S1) \Rightarrow \text{holds}(\text{S1}, \text{loaded}_\text{since}(B, A, T0)) \Leftrightarrow \text{holds}(\text{S1A}, \text{loaded}_\text{since}(B, A, T0))\).

**Proof:** From XD.10, E.19, E.21, K.4, and lemma B.19.

**Lemma B.40:**
\[
\begin{align*}
[\forall S0, S, S0A, SA] & \text{know}\_\text{acc}_\text{int}(A, S0, S, S0A, SA) \Rightarrow \Phi(A, SA, S0A) \lor \\
[\forall S0, S, S0A, SA] & \text{know}\_\text{acc}_\text{int}(A, S0, S, S0A, SA) \Rightarrow \neg\Phi(A, SA, S0A)
\end{align*}
\]

where \(\Phi\) is any of “el2\_\text{if}”, “el2\_\text{if}1”, “el2\_\text{if}2”, “el2\_\text{if}2\_\text{f}”, and “el2\_\text{if}3”.

(Agent \(A\) always knows whether any of the above conditions hold.)

**Proof:** From lemma B.21, B.14 together with E.20, E.21, and XD.6 through XD.11.

**Lemma B.41:**
\[
[AZ \neq \text{hero} \land \text{el2}\_\text{if}1(AZ, S2, S1)] \Rightarrow \\
[\text{know}_\text{next}_\text{step}(E, \text{el2}(AZ), AZ, S2, S1) \Leftrightarrow E=\text{do}(AZ, \text{call})].
\]

**Proof:** By X.6, the only next step of el2\((AZ)\) in \(S2\) is do\((AZ, \text{call})\). By E.15, this action is possible. By lemmas B.40 and B.18 and axiom E.19, \(AZ\) knows that this is the only next step and knows that it is possible.

**Lemma B.42:**
\[
[AZ \neq \text{hero} \land \text{el2}\_\text{if}2(AZ, S2, S1)] \Rightarrow \\
[\text{know}_\text{next}_\text{step}(E, \text{el2}(AZ), AZ, S2, S1) \Leftrightarrow E=\text{do}(AZ, \text{load}(b1))].
\]

**Proof:** Analogous to lemma B.41.

**Lemma B.43:**
\[
[\text{holds}(S1, \text{has}(AZ, B)) \land \neg\text{holds}(S2, \text{has}(AZ, B)) \land S1 < S2] \Rightarrow \\
\text{holds}(S2, \text{loaded}_\text{since}(B, AZ, \text{time}(S1))).
\]

**Proof:** By E.17 there exist \(S3, S4\) such that \(S3 < S2, S1 < S4, \text{ordered}(S2, S4)\) and occurs\((\text{do}(AZ, \text{load}(B)), S3, S4)\). By E.5 there exists \(SM < S4\) such that throughout\((SM, S4, \text{on}\_\text{elevator}(B))\). Let \(SA\) be the earlier of \(SM, S2\); thus \(SA < S4\) and \(SA \leq S2\). By E.9, holds\((\text{SA}, \text{elevator}\_\text{at}(AZ))\). Hence, by XD.10,
holds(S2, loaded, since(B, AZ, time(S1))

Lemma B.44:
\[ AZ \neq \text{hero} \land el2.g3(AZ, S2, S1) \]
\[ \text{know_next_step}(E, el2(AZ), AZ, S2, S1) \]
\[ \text{instance}(E, \text{inform}(AZ, \text{robots}, \text{loaded}, \text{since}(b1, AZ, \text{time}(S1))), S2) \]

Proof: Analogous to lemma B.41.

Lemma B.44.A:
\[ el2.g3(AZ, S2, S1) \]
\[ \exists E \text{ instance}(E, \text{inform}(AZ, \text{robots}, \text{loaded}, \text{since}(b1, AZ, \text{time}(S1))), S2) \land \text{feasible}(E, S2). \]

Proof: Let QL be the fluent \text{loaded}, since(b1, AZ, time(S1)). By axiom E.16, it is feasible for AZ to communicate to robots. By lemma B.39, AZ knows in S2 that QL. By C.1, inform(AZ, robots, QL) is feasible in S2. By C.4, know/select(AZ, inform(AZ, robots, QL), S2). The result follows from MD.1 and KHD.1.

Lemma B.45:
\[ AZ \neq \text{hero} \land \text{choice}(AZ, S1) \land 
\[ \neg el2.q11(AZ, S2, S1) \land 
\[ \neg el2.q22(AZ, S2, S1) \land 
\[ \neg el2.q33(AZ, S2, S1) \]
\[ \Rightarrow 
\[ \text{next_step}(E, el2(AZ), S1, S2) \]
\[ \Rightarrow 
\[ \text{action}(E, AZ) \land E \neq \text{do}(AZ, \text{unload}(b1)) \]


Lemma B.46:
\[ AZ \neq \text{hero} \land \text{choice}(AZ, S1) \land 
\[ \neg el2.q11(AZ, S2, S1) \land 
\[ \neg el2.q22(AZ, S2, S1) \land 
\[ \neg el2.q33(AZ, S2, S1) \]
\[ \Rightarrow 
\[ \text{know_next_step}(E, el2(AZ), AZ, S1, S2) \]
\[ \Rightarrow 
\[ \text{action}(E, AZ) \land E \neq \text{do}(AZ, \text{unload}(b1)) \land \text{feasible}(E, S2) \]

Proof: By lemma B.45, any action of AZ other than unload(b1) is a next step of el2(AZ). By lemmas B.17 and B.40, AZ knows that the conditions on the left-hand side of the implication hold, and (using lemma B.45) therefore knows that any action other than unload(b1) is next step of el2(AZ).

Lemma B.47: \neg abandon2(el2(AZ), AZ, hero, S1, S2)

Proof: By QD.4, if reserved(time(S2), AZ, hero), then \neg abandon2(el2(AZ), AZ, hero, S1, S2). Suppose that \neg reserved(time(S2), AZ, hero). By MD.2, MD.3, XD.7, XD.9, XD.11, none of the conditions el2.q11(AZ, S1, S2), el2.q22(AZ, S1, S2), el2.q33(AZ, S1, S2) hold. Let S1A and S2A be knowledge accessible from S1 and S2 respectively. By lemma B.40, none of the conditions el2.q11(AZ, S1A, S2A), el2.q22(AZ, S1A, S2A), el2.q33(AZ, S1A, S2A) hold. By X.6, any action other than “unload(b1)” is a next step of el2(AZ) in S2A. By E.22, X.9, this includes every action not governed by hero. The result follows from QD.4, PD.1.

Lemma B.48: terminates(el2(AZ), AZ, hero, S1, S2) \iff S2 > S1 \land \text{time}(S2) \geq \text{time}(S1) + \max_{el2b} \text{time}

Proof: By QD.5, el2(AZ) terminates in S2 if it is known to succeed or it is abandoned. From lemmas B.41, B.42, B.44, B.45, B.46, with definition QD.3, it follows that el2(AZ) is not abandoned type 1 in S2. Lemma B.47 states that el2(AZ) is not abandoned type 2 in S2. From X.5 and lemma B.14, el2(AZ) is known to succeed if \text{time}(S2) \geq \text{time}(S1) + \max_{el2b} \text{time}.

Lemma B.49:
\[ AZ \neq \text{hero} \land \text{working_on}(el2(AZ), AZ, hero, S0, S1) \]
\[ \neg \exists S2 \ S0 < S2 < S1 \land \text{leads toward}(\text{do}(AZ, \text{unload}(b1)), S2, S1). \]
Proof: By X.6 do(AZ,unload(b1)) is never a next step of el2(AZ). The result follows from lemma B.30, PD.1, and K.1.

Lemma B.50:
\[ \text{holds}(S1,\text{loaded}\text{.since}(b1,A2,\text{time}(S0))) \land \\
\forall AZ \; \; AZ \neq \text{hero} \Rightarrow \text{working.on}(el2(AZ),AZ,\text{hero},S0,S1)) \Rightarrow \\
\text{holds}(S1,\text{on.elevator}(b1)) \lor \text{holds}(S1,\text{has}(\text{hero},b1)). \]

Proof: By E.12, in S1, either b1 is on the elevator or some agent has b1. By XD.10 there exists a situation SA between S0 and S1 such that in SA, b1 is on the elevator, the elevator is at A2, and A2 is not engaged in unloading b1. By E.18, an agent other than hero can come to have b1 between SA and S1 only if an action "unload(b1)" occurs in an interval intersecting [SA, S1]. By lemma B.49, no action "do(AZ,unload(b1))" begins at an interval between S0 and S1; and by construction of SA, any action "do(AZ,unload(b1))" begun before S0 must be completed no later than SA. Hence, no such action occurs in an interval intersecting [SA, S1].

Lemma B.51:
\[ AZ \neq \text{hero} \land \text{accepts.req}(el2(AZ),AZ,\text{hero},S1) \land S2 \geq S1 \land \\
\text{soc.poss}(S2) \land \text{time}(S2) < \text{time}(S1) + \max el2b.time \Rightarrow \\
\text{working.on}(el2(AZ),AZ,\text{hero},S1,S2). \]

Proof: Let SM be any situation such that S1 \leq SM \leq S2. Then by T.16, \text{time}(SM) \leq \text{time}(S2) < \text{time}(S1) + \max el2b.time. By lemma B.48, \neg terminates(el2(AZ),AZ,\text{hero},S1,SM).

By QD.9, attempt.toward(el2(AZ),AZ,\text{hero},S1,S2). By QD.8, since \neg terminates(el2(AZ),AZ,\text{hero},S1,SM) for any SM between S1 and S2, it follows that begin_plan(el2(AZ),AZ,\text{hero},S1,S2). By Q.5, working.on(el2(AZ),AZ,AR,S1,S2).

Lemma B.52:
\[ AZ \neq \text{hero} \land \text{accepts.req}(el2(AZ),AZ,\text{hero},S1) \land S2 \geq S1 \land \text{soc.poss}(S2) \Rightarrow \\
\text{working.on}(el2(AZ),AZ,\text{hero},S1,S2) \iff \text{time}(S2) < \text{time}(S1) + \max el2b.time]. \]

Proof: The implication "working.on(el2(AZ),AZ,\text{hero},S1,S2) \Rightarrow \text{time}(S2) < \text{time}(S1) + \max el2b.time" follows directly from Q.5 and Lemma B.48. The full result thus follows from B.51.

Definition BD.5: leads_towards1(E, S, I) \equiv \exists S2 \; \text{occurs}(E, S, S2) \land [S2 \lt \text{start}(I) \lor \text{elt}(S2, I)].
(There is an occurrence of event E starting in S on the same time line as u-interval I.)

Lemma B.53:
\[ \text{soc.poss.int}(I) \land \text{elt}(S1, I) \land \text{working.on}(P, AC, AR, S0, S1) \land \text{choice}(A, S1) \Rightarrow \\
\exists E \; \text{know\_next\_step}(E, P, AC, S0, S1) \land \text{leads\_towards1}(E, S1, I). \]

Proof: From B.32, BD.4, BD.5.

Lemma B.54:
\[ AZ \neq \text{hero} \land \text{working.on}(el2(AZ), AZ, \text{hero}, S0, S1) \land \text{elt}(A1, AZ, S1, S0) \land \text{elt}(S1, I) \land \text{soc.poss.int}(I) \Rightarrow \\
\text{leads\_towards1}(do(AZ, call), S1, I) \]

Proof: From B.53, B.41.

Lemma B.55:
\[ AZ \neq \text{hero} \land \text{working.on}(el2(AZ), AZ, \text{hero}, S0, S1) \land \text{elt}(S1, I) \land \text{soc.poss.int}(I) \Rightarrow \\
\text{leads\_towards1}(do(AZ, load(b1)), S1, I) \]

Proof: From B.54, B.42.

Lemma B.56:
[AZ ≠ hero ∧ working on el2(AZ), AZ, hero, S0, S1) ∧ el2₂q3(AZ, S1, S0) ∧ elt(S1, I) ∧ soc pos int(I)] ⇒
leads towards1 (inform(AZ, robots, loaded since (b1, time(S0))), S1, I)

Proof: From B.53, B.44.A.

**Lemma B.57:**

\[ [AZ ≠ hero ∧ accepts req(el2(AZ), AZ, hero, S0) ∧ el2₂q2(AZ, S1, S0) ∧
reserved block(time(S1), AZ, hero, max action time) ∧
time(S1) + max action time ⩽ time(S0) + max el2b time ∧
soc pos int(I) ∧ elt(S0, I) ∧ elt(S1, I)] ⇒
∃S3, S4 elt(S4, I) ∧ time(S3) ⩽ time(S1) + max action time ∧
leads towards1 (inform(AZ, robots, loaded since (b1, time(S0))), S1, I) \]

Proof: By lemma B.52, working on el2(AZ), AZ, hero, S0, S1). By lemma B.55 there exists S2 in I such that occurs (do(AZ, load(b1))), S1, S2). By M.1, time(S2) ⩽ time(S1) + max action time ⩽ time(S0) + max el2b time. By lemma B.51, working on el2(AZ), AZ, hero, S0, S2). By E.5 and E.9 there exists SM such that S1 < SM < S2, holds(SM, on elevator(b1)), and by E.8, holds(SM, elevator at (AZ)). Thus by XD.12, holds(S2, loaded since (b1, AZ, time(S0))). By lemma B.9, choice(AZ, S2). By QD.1, reserved(time(S2), AZ, hero). Let S3 be the earliest time between S0 and S2 such that holds(S3, loaded since (b1, AZ, time(S0))), choice(AZ, S3), and reserved(time(S3), AZ, hero)). Then el2₂q3(AZ, S3, S0). The result then follows from lemma B.56.

**Lemma B.58:**

\[ [AZ ≠ hero ∧ accepts req(el2(AZ), AZ, hero, S1) ∧ holds(S1, has(AZ, b1)) ∧ soc pos int(I) ∧
elt(S1, I)] ⇒
∃S2, S3, S4 elt(S4, I) ∧ time(S3) ⩽ time(S1) + delay time + min reserve block ∧
leads towards1 (inform(AZ, robots, loaded since (b1, time(S0))), S1, I). \]

(If, in situation S1, AZ has the package and AZ accepts the request el2 broadcast by the hero, then within the time max el2 time, AZ will inform the hero that the package has been on the elevator at some time later than the broadcast.)

Proof: Let az, s1, i1 satisfy the left-hand side of the above implication.

Let t5 be the first time such that t5 ⩾ time(s1) and reserved block(t5, az, hero, 4 * max action time + max elevator wait). (The notation “4 * max action time” here and similar notations below should be taken as syntactic sugar for “max action time + max action time + max action time + max action time”. We do not have to introduce a general multiplication operator.) By Q.2 and X.7, such a t5 exists and t5 ⩽ t1 + delay time. Using lemma B.7, let s5 be a situation such that elt(s5, i1) and time(s5)=t5. Let s6 be the first situation after s5 in i1 such that choice(az, s6) (lemma B.13). By M.1, time(s6) ⩽ time(s5) + max action time, so by lemma B.27 reserved block(time(s6), az, hero, 3 * max action time + max elevator wait).

We now have a hierarchical case analysis.

**Case 1:** Suppose that holds(s6, has(az, b1)) and ~holds(s6, elevator at (az)). Then by XD.8, holds(s6, el₂q₁, f(az)), and by XD.9, el₂q₁(az, s6, s6). By lemma B.54, there is a situation s7 in i1 such that occurs (do(az, call), s6, s7). Using lemma B.7, let s8 be the situation in i1 such that time(s8) = time(s7) + max elevator wait. Note that, by lemma B.27 and axiom M.1, reserved block(time(s8), az, hero, 2 * max action time).

By E.4 and FD.6, there is a situation s9 in i1 such that that s7 ⩽ s8 and holds(s9, elevator at (az)). We have reserved block(time(s9), az, hero, 2 * max action time). By lemma B.13 there is a situation s10 in i1 such that choice(az, s10) within time max action time of time(s9). By lemma B.27 reserved block(time(s10), az, hero, max action time).
Let $s_{11}$ be the first situation such that $s_1 \leq s_{11} \leq s_{10}$, holds($s_{11}$, $\text{elevator at}(az)$), choice($az,s_{11}$) and reserved(block($time(s_{11})$, $az$, hero, max_action_time)).

There are now two cases to consider:

**Case 1.1:** Suppose that holds($s_{11}$, has($az$, $b_1$)). Then $el_2 \q_2(az,s_{11},s_0)$, so the result follows from lemma B.57.

**Case 1.2:** Suppose that $\neg$holds($s_{11}$, has($az$, $b_1$)). Then by lemma B.43, holds($s_{11}$, $\text{loaded since}(b_1,az, time(s_1))$). Let $s_{12}$ be the first situation such that $s_1 < s_{12} \leq s_{11}$, holds($s_{12}$, $\text{loaded since}(b_1,az, time(s_1))$), choice($az,s_{12}$), and reserved($time(s_{12})$, $az$, hero). Then $el_2 \q_3(az,s_{12},s_1)$. The result then follows from lemma B.56.

**Case 2:** Suppose that holds($s_6$, has($az$, $b_1$)) and holds($s_6$, $\text{elevator at}(az)$). The proof continues in the same way as in case 1 from situation $s_9$ onward.

**Case 3:** Suppose that $\neg$holds($s_6$, has($az$, $b_1$)). The proof continues in the same way as in case 1.2.

**Lemma B.59:**

$[AZ \not= \text{hero} \land \text{accepts req}(el_2(AZ), AZ, \text{hero}, S_1) \land \text{holds}(\text{S}_1, \text{elevator at}(AZ)) \land \text{holds}(\text{S}_1, \text{on elevator}(b_1)) \land \text{elt}([S_1, I] \land \text{soc poss int}(I)) \Rightarrow \exists_{S_2,S_3,Z} S_1 < S_2 < S_3 \land \text{elt}([S_3, I]) \land time(S_3) \leq time(S_1) + \text{delay time} + \text{min reserve block} \land \text{occurs(inform}(AZ, \text{robots}, \text{loaded since}(b_1, time(S_0))), S_2, S_3)$.

**Proof:** Let $az,s_{11},i_{11},s_5,s_6$ be the same as in the proof of B.58. By XC.11, holds($s_6$, $\text{loaded since}(b_1,az, time(s_1))$). The proof then continues as in Case 1 of lemma B.52.

**Validation of Plan el1**

**Lemma B.60:**

$\forall S_0,S \ S_0 < S \Rightarrow$

$\forall S_0,A,S \ [k \text{acc int}(hero,S_0, S, S_0 A, S A) \Rightarrow \Phi(S_0, S_0 A)] \lor$

$\forall S_0,A,S \ [k \text{acc int}(hero,S_0, S, S_0 A, S A) \Rightarrow \neg \Phi(S_0, S_0 A)]$

where $\Phi$ is any of the relations “$el_1 \q_1$”, “$el_1 \q_2a$”, “$el_1 \q_3$”, or “$el_1 \q_2$”.

(The hero always knows whether any of the above conditions hold.)

**Proof:** From lemmas B.14, B.21 together with K.3, E.19, E.21, FD.3, XD.1 through XD.5.

**Lemma B.61:**

$el_1 \q_1(S_1, S_0) \Rightarrow$

$[\text{know next step}(E,el_1,hero,S_1, S_0) \Leftrightarrow \text{instance}(E, \text{broadcast req}(hero, \text{robots}, r_2), S_1)] \land$

$[\text{exec cont}(E,el_1,hero,hero,S_1, S_0) \Leftrightarrow \text{instance}(E, \text{broadcast req}(hero, \text{robots}, r_2), S_1)]$

**Proof:** By XD.2, MD.2, MD.3, $S_1$ is a choice point for hero. By X.2, the only next steps of $el_1$ in $S_1$ are the instances of $\text{broadcast req}(hero, \text{robots}, r_2)$. By lemma B.60 the hero knows that these are the only next steps for $el_1$ in $S_1$. By E.22 and Q.3, no one else governs these actions. Hence by QD.2 these are is the only executable continuation of $el_1$ in $S_1$.

**Lemma B.62:**

$el_1 \q_2(S_1, S_0) \Rightarrow$

$[\text{know next step}(E,el_1,hero,S_0, S_0) \Leftrightarrow E= \text{do}(hero, \text{call})] \land$

$[\text{exec cont}(E,el_1,hero,hero,S_1, S_0) \Leftrightarrow E= \text{do}(hero, \text{call})].$

**Proof:** Analogous to lemma B.61.

**Lemma B.63:**
el1_\sigma_3(S_1, S_0) \Rightarrow \\
[\text{know\_next\_step}(E, el1, hero, S_0, S_0) \Leftrightarrow E=\text{do}(hero, \text{unload}(b_1))] \land \\
[\text{exec\_cont}(E, el1, hero, hero, S_1, S_0) \Leftrightarrow E=\text{do}(hero, \text{unload}(b_1))] .

\textbf{Proof:} Analogous to lemma B.61.

\textbf{Lemma B.64:} \\
[\text{working\_on}(el1, hero, hero, S_0, S_1) \land \text{elt}(S_1, I) \land \text{soc\_poss\_int}(I) \land el1_\sigma_1(S_1, S_0)] \Rightarrow \\
\text{leads\_towards}_1(\text{broadcast\_req}(hero, robots, r_2), S_1, I).

\textbf{Proof:} From B.53, B.61.

\textbf{Lemma B.65:} \\
[\text{working\_on}(el1, hero, hero, S_0, S_1) \land \text{elt}(S_1, I) \land \text{soc\_poss\_int}(I) \land el1_\sigma_2(S_1, S_0)] \Rightarrow \\
\text{leads\_towards}_1(\text{do}(hero, \text{call}), S_1, I).

\textbf{Proof:} From B.53, B.62.

\textbf{Lemma B.66:} \\
[\text{working\_on}(el1, hero, hero, S_0, S_1) \land \text{elt}(S_1, I) \land \text{soc\_poss\_int}(I) \land el1_\sigma_3(S_1, S_0)] \Rightarrow \\
\text{leads\_towards}_1(\text{do}(hero, \text{unload}(b_1)), S_1, I).

\textbf{Proof:} From B.53, B.63.

\textbf{Lemma B.67:} \\
\text{begin\_plan}(el1, hero, hero, S_0, S_1) \land \text{terminates}(el1, hero, hero, S_0, S_1) \Rightarrow \\
\text{know\_succeeds}(el1, hero, S_0, S_1).

(Plan el1 can only terminates with success.)

\textbf{Proof:} Suppose that \text{begin}(el1, hero, hero, S_0, S_1) and \neg \text{know\_succeeds}(el1, hero, hero, S_0, S_1). We wish to show that el1 does not terminate in S_1. There are two cases to consider:

\textbf{Case 1:} S_1 = S_0 or el1_\sigma_2(S_1, S_0) or el1_\sigma_3(S_1, S_0). By lemmas B.61, B.62, B.63 there is an executable continuation for el1 in S_1; hence by QD.2, QD.3, QD.5, el1 does not terminate in S_1.

\textbf{Case 2:} S_1 \neq S_0 and \neg el1_\sigma_2(S_1, S_0) and \neg el1_\sigma_3(S_1, S_0). If S_1 is not a choice point for the hero, then el1 does not terminate in S_1 (QD.3, QD.4, QD.5), so assume that S_1 is a choice point. By X.2, any action E of the hero is a next step of el1. By lemma B.60 the hero knows that S_1 \neq S_0, \neg el1_\sigma_2(S_1, S_0), and \neg el1_\sigma_3(S_1, S_0), so he knows that any action of his is a next step. In particular, as “wait” is always possible, he knows that “wait” is a possible next step (axioms A.7 and PD.1). Therefore, if time(s_1) is reserved for hero by hero, then “Wait” is an executable continuation of el1, so abandon1 is not satisfied (QD.2, QD.3). If time(s_1) is not reserved for hero by hero, then abandon2 is not satisfied (QD.4). Since, by assumption, \text{know\_succeeds} is not satisfied, it follows from QD.5 that the plan does not terminate.

\textbf{Lemma B.68:} \\
el1_\sigma_1(AZ, S_2, S_1) \Rightarrow \\
\exists E \text{ instance}(E, \text{broadcast\_req}(AZ, robots, r_2), S_2) \land \text{feasible}(E, S_2).

\textbf{Proof:} By axiom E.16, it is feasible for AZ to communicate to robots. By C.5, broadcast(AZ, robots, r_2) is feasible in S_2. By C.6, know\_how(AZ, broadcast(AZ, robots, r_2), S_2). The result follows from MD.1 and KHD.1.

\textbf{Lemma B.69:} \\
[\text{working\_on}(el1, hero, hero, S_0, S_0) \land \text{elt}(S_0, I_0) \land \text{soc\_poss\_int}(I_0) \land \\
\forall_{AZ, r_2} AZ \neq hero \Rightarrow \neg \text{working\_on}(P_2, AZ, hero, S_0, S_0)] \Rightarrow \\
\exists S_Z S_Z \geq S_0 \land \text{elt}(S_Z, I) \land \text{completes}(el1, hero, hero, S_0, S_Z).

\textbf{Proof:}
Assume that s0 and i0 satisfy the left hand of the implication. Let s1 be the first situation after s0 in i0 such that reserved(time(s1),hero,hero) and choice(hero,s1). By Q.2, QD.1, X.7, such an s1 will occur in i0 within time at most delay\_time + max\_action\_time of s0. By XD.3, el1\_q1(s1,s0). By lemma B.68, there is a situation s2 in i0 such that occurs(broadcast\_req(\hero,\robots,r2),s1,s2). By S.6, the event request(\hero,A2 assignment(r2,A2)) occurs from s1 to s2 for every agent A2 ≠ hero.

By lemma B.67 and B.36, either el1 has completed before s2 or hero is still working on el1 in s2. If el1 has completed, then that completes the proof, so assume that el1 has not completed. By X.2 and lemma B.33, hero does not issue any broadcasts other than r2 between s0 and s2. By S.7, hero does not make any requests of A2 between s0 and s2. By Q.6, A2 has not accepted any other requests of hero between s0 and s2. By Q.5, A2 is not working on any plans of hero at s2. By Q.6, A2 accepts the request assignment(r2,A2) = el2(A2).

By E.12, E.13 there is an agent az such that, in s2, either az has b1 or the elevator is at az and b1 is loaded on the elevator. By lemmas B.58, B.59 there exist situations s3, s4 in i0 such that occurs(inform(az, \robots, loaded\_since(b1,az,time(s0))),s3,s4), and s4 in i0. By C.2, CK.1, the hero knows in s4 that a2 has informed him of this fact; that is, in every situation S4B accessible from s4, it is the case that there exists an S4B accessible from s4a and S3B < S4B such that occurs(inform(az, \robots, loaded\_since(b1,az,time(s0))),S3B,S4B) By C.1, K.1, in any such S3B it is the case that loaded\_since(b1,az,time(s0)).

Let s5 be the first situation after s4 in i0 such that reserved\_block(time(s5), hero, 3*max\_action\_time + max\_elevator\_wait). By Q.2, X.7, time(s5) ≤ time(s4) + delay\_time. Suppose that k\_acc(hero,s5,S5B) accessible from s5. By K.4, there exists S4B ≤ S5B such that k\_acc(hero,s4,S4B). By lemma B.50, b1 is on the elevator in S5B. Thus by XD.1 holds(s5, know\_loaded(\hero,b1)). Let s6 be the first opportunity after s0 in which know\_loaded(\hero,b1); then time(s6) ≤ time(s5) + max\_action\_time and reserved\_block(time(s6), hero, 2*max\_action\_time + max\_elevator\_wait).

There are now two cases to consider:

Case 1: Suppose that el1\_q3(S,s0) does not hold for any S between s0 and s6. Then el1\_q2(s6,s0) (XD.4, XD.5). By lemma B.62 there exists s7 in i0 such that occurs(do(\hero,\commit(\hero,el1)),s0a,s1a), elt(s1a,i0), and soc\_poss\_int(i0). By X.13 :9 P;AC;SX working on(P, AC, SX, s0a); that is, in s0a no one including hero is working on any plans of hero’s. Since no other commit or broadcast actions occur between s0a and s1a (axioms A.1, A.2), no other requests occur (S.7) or are accepted (Q.6); hence, in s1a still no one is working on any plans of hero’s (lemma B.31). By lemma B.69, el1 completes in i0.

Case 2: Suppose that el1\_q3(S,s0) holds for some S between s0 and s6. Then the proof continues as in Case 1, from s10 on.

Lemma B.70: k\_acc(\hero,s0,SOA) ⇒ executable(el1,\hero,SOA)

Proof: Assume that k\_acc(\hero,s0,s0a), occurs(do(\hero,\commit(\hero,el1)),s0a,s1a), elt(s1a,i0), and soc\_poss\_int(i0). By X.13 ⇒3 P,AC,SX working on(\hero,\AC,\SO,X,s0a); that is, in s0a no one including hero is working on any plans of his. Since no other commit or broadcast actions occur between s0a and s1a (axioms A.1, A.2), no other requests occur (S.7) or are accepted (Q.6); hence, in s1a still no one is working on any plans of hero’s (lemma B.31). By lemma B.69, el1 completes in i0. Therefore, el1 is executable in s0a (Q.11).
Theorem B.71: know\_achievable(has(hero,b1),el1,hero,s0).

Proof: From lemma B.70 we have k\_acc(hero,s0,S0A) \Rightarrow executable(el1,hero,S0A). From X.1, QD.8, PD.2, K.1, we have completes(el1,hero,hero,S0A,S1A) \Rightarrow holds(S1A,has(hero,b1)). The result follows from QD.16. \qed